UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

GENESCO INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 3:13-0202
	)	Judge William J. Haynes, Jr.
VISA U.S.A. INC; VISA INC.; and VISA INTERNATIONAL SERVICE ASSOCIATION,	)	JURY DEMAND
	)	
Defendants.	)	

AFFIDAVIT OF SETH HARRINGTON IN SUPPORT OF PLAINTIFF GENESCO INC.'S MOTION FOR PROTECTIVE ORDER

I, Seth C. Harrington, Esq., state as follows:

1. I am over the age of eighteen.

2. I am a member of the bar of the Commonwealth of Massachusetts. I am an associate at the law firm of Ropes & Gray LLP, which represents Plaintiff Genesco Inc. ("Genesco") in the above-captioned action.

3. The information contained in this affidavit is true and correct to the best of my personal knowledge.

4. A true and correct copy of the Notice of Deposition of Genesco Inc. Pursuant to Fed. R. Civ. P. 30(b)(6) (the "Deposition Notice") is attached hereto as Exhibit A.

5. A true and correct copy of excerpts from the *Visa International Operating Regulations*, October 15, 2010, is attached hereto as Exhibit B.

6. VIOR ID# 010410-010410-0009032 states that "a U.S. Member that fails to comply with the requirements of the Cardholder Information Security Program is assessed a fine,

as specified in the table below and the *Account Information Security Program Guide*." *See* Ex. B hereto at 3.

7. VIOR ID# 081010-010410-0000880 states that "A U.S. Member is compensated for a portion of its counterfeit fraud losses incurred as the result of a Magnetic-Stripe Data account compromise event. The Counterfeit Fraud Recovery process is initiated by Visa when: An account compromise event occurs; A Compromised Account Management System (CAMS) Alert, or multiple CAMS Alerts for the same account compromise event, is sent to affected Members; Effective for Qualifying CAMS Events that occur on or before 30 June 2010, the account compromise event involves at least 10,000 Account Numbers; Effective for Qualifying CAMS Events that occur on or after 1 July 2010, the account compromise event involves at least 10,000 Account Numbers **and** a combined total of US $100,000 or more recovery for all Issuers involved in the event; At least one of the following: The full contents of any track on the Magnetic Stripe was stored subsequent to Authorization of a Transaction, A violation of the Payment Card Industry Data Security Standard (PCI DSS) could have allowed a compromise of the full contents of any track on the Magnetic Stripe, A violation of the PIN Management Requirements Documents could have allowed a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to Authorization; Incremental fraud is attributed to the particular account compromise event." *See* Ex. B hereto at 6-7.

8. VIOR ID# 081010-010410-0000890 states that "A U.S. Member enrolled in the Operating Expense Recovery process is compensated for a portion of its operating expenses incurred as the result of a Magnetic-Stripe Data account compromise event. The Operating Expense Recovery process is initiated by Visa when: An account compromise event occurs; A CAMS Alert, or multiple CAMS Alerts for the same account compromise event, is sent to

affected Members; Effective for Qualifying CAMS Events that occur on or before 30 June 2010, the account compromise event involves at least 10,000 Account Numbers; Effective for Qualifying CAMS Events that occur on or after 1 July 2010, the account compromise event involves at least 10,000 Account Numbers **and** a combined total of US $100,000 or more recovery for all Issuers involved in the event; At least one of the following: The full contents of any track on the Magnetic Stripe was stored subsequent to Authorization of a Transaction, A violation of the Payment Card Industry Data Security Standard (PCI DSS) could have allowed a compromise of the full contents of any track on the Magnetic Stripe, A violation of the PIN Management Requirements Documents could have allowed a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to Authorization." *See* Ex. B hereto at 8-9.

9. VIOR ID# 010410-010410-0000867 states that "Visa will determine data compromise event eligibility based on: Forensic confirmation or preponderance of evidence that a breach exists; A violation of the Payment Card Industry Data Security Standard (PCI DSS) occurred that could allow a compromise of account data; Full Magnetic Stripe counterfeit fraud occurred on a portion of exposed Account Numbers; A minimum of 10,000 Account Numbers were exposed and a minimum of US $100,000 in Magnetic Stripe counterfeit fraud occurred during the data compromise event time period." *See* Ex. B hereto at 11.

10. A true and correct copy of a letter from Visa to Wells Fargo Bank dated May 31, 2011 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit C.

11. A true and correct copy of a letter from Visa to Fifth Third Bank dated May 31, 2011 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit D.

12. A true and correct copy of a letter from Visa to Wells Fargo Merchant Services, LLC dated November 8, 2011 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit E.

13. A true and correct copy of a document entitled Visa Account Data Compromise Recovery (ADCR) Qualification Summary dated November 7, 2011 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit F.

14. A true and correct copy of a letter from Visa to Wells Fargo Merchant Services, LLC dated November 8, 2011 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit G.

15. A true and correct copy of a document entitled Visa Data Compromise Recovery Solution (DCRS - International) Qualification Summary dated November 7, 2011 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit H.

16. A true and correct copy of a letter from Visa to Fifth Third Bank dated November 8, 2011 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit I.

17. A true and correct copy of a document entitled Visa Account Data Compromise Recovery (ADCR) Qualification Summary dated November 7, 2011submitted under seal

pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit J.

18. Subsequent to the discovery of the Intrusion, Visa conducted an almost six-month investigation for the purpose of determining whether, by reason of the Intrusion, Visa should impose fines and issuer reimbursement assessments on the Acquiring Banks pursuant to these VIOR provisions. *See* Exs. C, D ("At this time, the investigation concerning the May 2010 incident involving Genesco is now complete"); Exs. E, I ("The Account Data Compromise Recovery (ADCR) Review Team has reviewed the facts of case US-2010-992 related to Genesco and has determined that it **qualifies** for ADCR processing. The attached 'Qualification Summary' documents the forensic and analytic evidence used to determine ADCR qualification in this case."); Ex. G ("The Data Compromise Recovery Solution (DCRS) Review Team has reviewed the facts of case US-2010-992 related to Genesco and has determined that it **qualifies** for DCRS processing. The attached 'Qualification Summary' documents the forensic and analytic evidence used to determine ADCR qualification in this case."); *see also* Exs. F, H, and J at 1-8 (summarizing Visa's investigation).

19. Visa determined to impose the fines and issuer reimbursement assessments based on the alleged "PCI DSS Violations" at the time of the Intrusion ostensibly found in the Trustwave Report. *See* Ex. F at 6-7 ("There were 3 PCI violations (Forensic Report, p. 37 … The PCI DSS Violations indicated as 'Not In Place' on page 7 could have allowed a compromise to occur."); Ex. H at 6-7 (same); Ex. J at 6-7 (same).

20. A true and correct copy of What To Do If Compromised Visa Inc. Fraud Control and Investigations Procedures Version 2.0 (Global) Effective February 2010 Visa Public is attached hereto as Exhibit K.

21. Under the VIOR, Visa may require an acquirer or its merchant to conduct a investigation of suspected or confirmed loss, theft, or compromise of Visa account information by engaging a forensic investigator approved by Visa, referred to as either a Qualified Incident Response Assessor ("QIRA"), Qualified Forensic Investigator ("QFI"), or PCI Forensic Investigator ("PFI"). *See* Ex. B hereto at 2, VIOR ID# 010410-010410-0007124 ("If required, the Member or its agent must … engage a Qualified Incident Response Assessor (QIRA) or Qualified Forensic Investigator (QFI)").

22. The investigator's role is to determine (1) whether a data security breach has occurred, (2) whether and to what extent payment card data was compromised in the course of the data security breach, and (3) whether the breached entity bears responsibility for the compromise of payment card data by reason of non-compliance with PCI DSS. *See* PCI PFI Program Guide v2.0 at 12-15 available at https://www.pcisecuritystandards.org/documents/PFI_Program_Guide.pdf (last visited 10/15/13); Ex. K hereto at 18 ("A Visa client or compromised entity must ensure that only a Visa-approved Qualified Incident Response Assessor (QIRA) is engaged to perform a forensic investigation. It is the compromised entity's responsibility to pay for the cost of the forensic investigation. Visa has the right to engage a QIRA to perform a forensic investigation as it deems appropriate, and will assess all investigative costs to the Visa Member in addition to any fine that may be applicable. All QIRAs are required to adhere to the following forensic investigation guidelines. Visa clients can also use these guidelines to monitor the work by the QIRA. Visa will **NOT** accept forensic reports from non-approved forensic companies. QIRAs are required to release forensic reports and findings to Visa."); *id.* at 21 ("Determine what applicable PCI

security requirements apply … [and] which PCI DSS requirements and sub-requirements contributed to the breach of cardholder data.").

23. The investigator is contractually required to "[e]nsure that each PFI Investigation is not and shall not be directed or controlled in any way by the subject Compromised Entity," "[u]pon request of any affected Participating Payment Brand, make drafts of applicable PFI Reports and related work papers available to such Participating Payment Brand," and "[u]pon request of any affected Participating Payment Brand, reasonably cooperate with such Participating Payment Brand in such Participating Payment Brand's investigation of such Security Issue." Supplement for PCI Forensic Investigators (PFIs), Version 2.0, at 21, available at https://www.pcisecuritystandards.org/documents/PFI_Supplemental_Requirements_v2.0.pdf. (last visited 10/15/13).

24. The Payment Card Industry Security Standards Council, which is led by a policy-setting Executive Committee comprised of one representative from each of the five card brands, has approved only 22 firms, including Trustwave, to conduct forensic investigations of a data security breach involving payment card data. *See* "List of Approved PCI Forensic Investigators" available at https://www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php (last visited 10/15/13). Each firm must be evaluated and re-approved annually by the PCI SSC. Supplement for PCI Forensic Investigators (PFIs), Version 2.0, at 22, available at https://www.pcisecuritystandards.org/documents/PFI_Supplemental_Requirements_v2.0.pdf. (last visited 10/15/13).

25. A true and correct copy of the Incident Response Final Report issued by Trustwave to Visa on January 27, 2011 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit L.

26. On January 27, 2011, Trustwave delivered to Visa the Trustwave Report. Ex. L at 2. The Trustwave Report found (erroneously, in Genesco's view) that at the time of the Intrusion Genesco was in violation of four of the 244 PCI DSS requirements. *Id.* at 37. However, the Trustwave Report further found that Genesco was in full compliance with each and every one of the PCI DSS's other 240 requirements at the time of the Intrusion. *Id.*

27. A true and correct copy of Visa Defendants' Amended Response to Plaintiff Genesco Inc.'s First Set of Interrogatories submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit M.

28. A true and correct copy of the Affidavit of Matthew Johnson is attached hereto as Exhibit N.

29. A true and correct copy of Visa's review of Genesco's PCI DSS violations by Ingrid Beierly dated July 11, 2011 (VISA005334-5335) submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit O.

30. A true and correct copy of E-mail from Patrick Cleary to John Askins dated January 31, 2011 (VISA000693-694) submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit P.

31. A true and correct copy of Visa's First Request for Production of Documents is attached hereto as Exhibit Q.

32. A true and correct copy of Visa First Set of Interrogatories is attached hereto as Exhibit R.

33. A true and correct copy of Visa First Set of Requests for Admission is attached hereto as Exhibit S.

34. Visa's written discovery requests were not focused specifically on the four PCI DSS requirements that Trustwave found to have been violated and on which Visa relied in imposing the Fines and Assessments but rather inquired generally into Genesco's PCI DSS compliance and information security posture at the time of the Intrusion. *See, e.g.*, Ex. Q hereto at 8 ("All DOCUMENTS relating to YOUR compliance or non-compliance with the CARDHOLDER DATA SECURITY REQUIREMENTS, including without limitation any and all internal reports and external COMMUNICATIONS, for the time period from January 1, 2007 to present."); *id.* at 9 ("All DOCUMENTS related to the PERSON(S) that provided YOU with any component or services in connection with the GENESCO PAYMENT PROCESSING NETWORK in use during the INTRUSION through the present time); Ex. R hereto at 9 ("If YOU contend that GENESCO was compliant with the PCI DSS at all times DURING the INTRUSION, state all facts in support of this contention."); *id.* at 10 ("Identify everything GENESCO did to change, modify or alter in any way its corporate wide area network (WAN) computer system or its CARDHOLDER DATA ENVIRONMENT computer system after the INTRUSION, and state all facts as to why such changes were made."); Ex. S hereto at 9 ("Admit that GENESCO made changes to its security measures after the INTRUSION.")

35. A true and correct copy of Genesco's Objections to Visa First Request for Production of Documents is attached hereto as Exhibit T.

36. A true and correct copy of Genesco's Objections to Visa First Set of Interrogatories submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit U.

37. A true and correct copy of Genesco's Objections to Visa First Set of Requests for Admission submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit V.

38. A true and correct copy of a letter from Ropes & Gray LLP to O'Melveny and Myers dated August 9, 2013 is attached hereto as Exhibit W.

39. Genesco uniformly objected to Visa's discovery requests inquiring generally into Genesco's PCI DSS compliance and information security posture at the time of the Intrusion and thereafter. *See* Ex. T hereto at 11-16, 21-23; Ex. U hereto at 15-18; Ex. V hereto at 18. Specifically, Genesco objected on the ground that (1) Visa had no reasonable basis for believing that, and thus had no reasonable basis for taking discovery as to whether, at the time of the Intrusion Genesco was non-compliant with one of the 240 other PCI DSS requirements not relied upon by Visa in imposing the Fines and Assessments, (2) such evidence would be irrelevant to whether Visa acted lawfully in imposing the Fines and Assessments; and (3) such evidence would be inadmissible. *See, e.g.*, Ex. W at 2-4.

40. Counsel for Visa and Genesco have engaged in several meet and confer conferences relative to Visa's First Request for Production of Documents, Visa First Set of Interrogatories, Visa First Set of Requests for Admission.

41. Genesco agreed, notwithstanding its objections to Visa's discovery requests, to conduct a reasonable non-ESI search for and produce (if located in such search) (1) any documents reflecting Genesco's PCI DSS compliance policies in place during the period of the Intrusion, or any changes to such policies, including analyses, meeting minutes, or other reasonably identifiable documents discussing those policies or actual or potential changes in those policies and (2) any documents discussing Genesco's actual or potential non-compliance

with the PCI DSS and any other applicable cardholder account security requirements during the period of the Intrusion. Additionally, Genesco proposed conducting an ESI search for documents relating to Genesco's compliance or non-compliance with the PCI DSS generated prior to Genesco's retention of outside counsel to conduct an investigation of the Intrusion for the purpose of providing legal advice to Genesco regarding the Intrusion and in anticipation of litigation with the card brands and other persons arising out of the Intrusion.

42. A true and correct copy of Genesco Self-Assessment Questionnaire, dated September 10, 2009 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit X.

43. A true and correct copy of Genesco's Self-Assessment Questionnaire, dated November 24, 2010 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit Y.

44. The VIOR require a merchant of Genesco's size to validate compliance with the PCI DSS on an annual basis using a "Self-Assessment Questionnaire" that evaluates whether all applicable PCI DSS requirements are "in place." *See* "Merchant levels and compliance validation requirements defined" available at http://usa.visa.com/merchants/risk_management/cisp_merchants.html#anchor_3 (Last visited 10/15/13).

45. Genesco's Self-Assessment Questionnaire, dated September 10, 2009, found all applicable PCI DSS requirements to be "in place" as of the date of the assessment. *See* Ex. X.

46. Genesco's Self-Assessment Questionnaire, dated November 24, 2010, found all applicable PCI DSS requirements to be "in place" as of the date of the assessment. *See* Ex. Y.

47. A true and correct copy of a document entitled *Updated Account Data Compromise Recovery (ADCR) Frequently Asked Questions*, VRM 03.19.08 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit Z.

48. [REDACTED]

49. A true and correct copy of a document entitled *Data Compromise Recovery Solution*, Visa International Member Letter 21/07 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit AA.

50. [REDACTED]

51. A true and correct copy of a letter from Ropes & Gray LLP to O'Melveny and Myers dated September 6, 2013 submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013 is attached hereto as Exhibit BB.

52. As of the date of this motion, Visa has not identified any document upon which it intends to rely for the contractual authority to impose fines and assessments based upon facts that were not obtained during the course of Visa's investigation of an alleged account data compromise event and/or that were not relied upon by Visa in imposing such fines and assessments.

53. A true and correct copy of an E-mail dated October 22, 2010 from Joseph Majka to Giovanni Leoni (VISA000761) submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit CC.

54. A true and correct copy of an E-mail dated October 25, 2010 from John Askins to AssociationNotification@wellsfargo.com (VISA000762-763) submitted under seal pursuant to a Motion to Seal filed with the Court on October 17, 2013, is attached hereto as Exhibit DD.

55. [REDACTED]

56. A true and correct copy of a the Form 10-Q for Visa Inc. for the quarter ending June 30, 2013 is attached hereto as Exhibit EE.

57. After the meet and confer between counsel on October 11, 2013, Visa and Genesco agreed that Genesco's instant motion would be deemed timely if filed on or before October 17, 2013, with Visa's response in opposition due no later than October 24, 2013 and any reply in support by Genesco would be filed no later than October 29, 2013.

SWORN AND SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 16th DAY of October, 2013

Seth C. Harrington, Esq.

Sworn before me this 16th day of October, 2013:

Notary Public

My Commission Expires: 8/15/2019

Dated: October 16, 2013

MICHELLE F. FLAHERTY
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
August 15, 2019